January 14, 2003

Attn: Velica Steadman
United States Patent and Trademark Office
Office of Legislative and International Affairs
Room 902
2121 Crystal Drive
Arlington, VA 22202

Re: SIIA Comments and Request to Testify at Hearings on Technological Protection Systems for Digitized Copyrighted Works

Dear Ms. Steadman:

In response to the Federal Register notice dated December 3, 2002, entitled "Request for Written Comments and Notice of Hearings on Technological Protection Systems for Digitized Copyrighted Works" and published by the United States Patent and Trademark Office (PTO), the Software & Information Industry Association ("SIIA") hereby submits the following comments on behalf of its members.

SIIA is the principal trade association of the software and information industry and represents over 600 high-tech companies that develop and market software and electronic content for business, education, consumers, the Internet, and entertainment. SIIA members represent a wide range of business and user interests. In particular, numerous SIIA members:

- Create and develop new and valuable technological protection systems for use by others,

- Use technological protection systems to protect their proprietary software and content, and

- Purchase or license software and information products and other content and services that utilize technological protection systems.

Consequently, SIIA and our members are extremely interested in issues relating to the development and use of technological protection systems to protect copyrighted works.

Because the Federal Register notice is responsive to a requirement in the Technology, Education and Copyright Harmonization Act of 2001 (TEACH Act, P.L. No. 107-273) it is important to recognize that SIIA and our members have a significant interest in the use of technology in the educational environment. Many SIIA member software and content publishers provide educational software tools and digital curriculum to the K-12, higher education and corporate training markets. SIIA and our member companies believe that technology is critical to meeting the nation's education and training goals.

One of our major standards initiatives in this area is SIIA's Schools Interoperability Framework (SIF) initiative. Driven by more than 100 education technology providers and users seeking to revolutionize information management within the K-12 environment, the goal of SIF is to develop an open specification for ensuring that K-12 instructional and administrative software applications work together more effectively. SIF is not a product, but rather an industry-supported technical blueprint for K-12 software that will enable diverse applications to interact and share data efficiently, reliably and securely regardless of platform.

In light of our experience in the variety of markets in which our members operate, we find that on the whole technological protection systems have been developed and implemented reflecting market demands. Those demands have not and cannot be met by a one-size-fits-all business and technical solution. On the contrary, technological protection systems have been successful when they are appropriate to the circumstances of the market situation, taking into account user needs, the value of the information or content to be protected and the soundness of the business model. It is also clear that this is a dynamic market where changes in both technology and business models are evolving rapidly.

It is with this background information, and through these experiences, that SIIA provides its comments (below) on the three questions posed by the PTO in the Federal Register notice.

1. **What technological protection systems have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including any upgradeable and self-repairing systems?**

The functionality provided by technological protection systems basically fall into three categories:

> Access Control Functions: These functions control the user's right of entry to the protected content, e.g., encryption and/or authentication.
>
> Use Control Functions: These functions control how the user can interface with the protected content, e.g., read-only rights (the user is unable to print, save or distribute the content).
>
> Tracking Functions: These functions allow the content provider to track the subsequent use and/or distribution of its content online, e.g., watermarking and digital footprints.

Within each type of protection system, there are varying degrees of protection. For example, different types of access control systems include:

Type of Protection	**Level of Protection**
Encryption	High Level of Protection
Subscription	Medium Level of Protection
Registration/Password	Medium-Low Level of Protection
Click-through Agreement	Low Level of Protection

For systems using use control functions:

Type of Protection	**Level of Protection**
Read-only	High Level of Protection
Read & Print rights	Medium Level of Protection
Full Access	Low Level of Protection

For systems using tracking functions:

Type of Protection	**Level of Protection**
Watermarking/Digital Footprints	High Level of Protection
Online/electronic Clearinghouse	Medium Level of Protection
Voluntary User Compliance	Low Level of Protection

A technological protection system may include one or more of these functions. For example, a certain technological protection system may incorporate password access controls and read-only use controls to prevent wrongful access and wrongful re-distribution of the protected product. To some extent access control and use control functions may also be overlapping. For instance, access controls also serve as use controls since a user who does not have access to the content may not use it.

Digital technology can now make it easier than ever before to secure online copyright protection in many context. Technological protection systems enable copyright protection, distribution, usage and payment for digital content such as text, music, images or software via any electronic medium. Many companies have emerged that provide core technology for technical protection systems or serve as clearinghouses for use permissions for copyrighted content. These entities deliver technological protection solutions that implement sophisticated rights and permissions business models, combined with a back-office rights clearance infrastructure for managing rights.

It is not possible to identify each and every technological protection system that has been implemented, is available or has been proposed. We have provided in Appendix A, a list of technological protection system providers. This list includes a brief description of the technological protection systems they offer, as well as their contact information. Many of the technological protection system providers identified in Appendix A will no doubt be submitting comments to the PTO themselves. For those that do not, we urge the PTO, Copyright Office and other interested parties to learn more about the various technological protection systems that are available by accessing the websites of all the technological protection system providers possible.

Below is a brief overview of the technologies and applications, although not specific brand names, currently available in the marketplace and used primarily by the software and digital content publishers. The overview is provided by way of example and, like Appendix A, is not intended to be an exhaustive list of technological protection systems. Nor should this overview be construed to mean that SIIA believes that technological protections systems represent a complete solutions. While technological protection systems offer significant benefits to intellectual property owners, they are not a complete solution to the piracy problem. Lastly, while various technological protection systems are described, it is SIIA's view that education providers must work hand in hand with technological protection system providers to determine which method(s) of protection is best for their individual case, product or partnership and educational needs.

Subscriber Agreement

Subscriber agreements are the most common type of copyright control for certain works. Both rights-holders and authorized third-party distributors use subscriber agreements that allow clients to access content subject to various restrictions, the most common of which is limiting or prohibiting re-distribution to third parties. Users who wish to gain access to the copyrighted material must first accept the conditions of the comprehensive "terms of use" licenses included in the subscription process.

The challenge here is that nearly every subscriber now has the technological capability to re-distribute or even republish digitally. Publishers are faced with strictly and forcefully enforcing existing contractual limitations on re-distribution by subscribers or adapting their subscriber agreements to authorize re-distribution only under specified conditions. Whether publishers choose to license "infomediaries" (i.e., firms operating under license from copyright holders to act as aggregators and re-distributors of content) to manage the republishing of their content or preserve a direct contractual link with their subscribers, publishers and their licensees must pay increasingly close attention to the contracts and licenses they sign.

The good news is that the introduction of online agreements and digital rights management technologies can facilitate a wide range of options for the development of license agreements and procedures. Rights management in this case means harnessing these technologies to achieve the best fit with commercial aims and user requirements.

Rights Modeling

The most basic component of any technological protection system is the way it manages the user rights the copyright holder has granted each particular user. Rights models specify types of rights (e.g., print, view, play, copy, re-distribute), types of users who can acquire rights (e.g., subscriber, one-time user, student discount, site licensee), extent of rights (e.g., print X times, view for Y days, play for Z hours) and costs associated with each of those rights. These models are set in the metadata of the electronic transaction.[1] Some technological protection systems use these standard technologies, while others use proprietary rights-modeling schemes.

[1] Metadata is machine-understandable information used for web-based transactions.

There can be considerable granularity in the application of these rights models to suit specific business, product or market requirements. In one such model, the Protexis' rights-modeling scheme, rights are delivered or enabled through activation codes. These activation codes for access or enablement of protected content can be generated such that they are only useful for a predetermined period of time, for example. In this proprietary scheme, the activation codes are generated using product codes that are computer-dependent.

This same Protexis' nTitles system also employs a content protection scheme whereby user rights in terms of the availability of various functions provided in a software program can be controlled on a feature-specific, application-specific, release-specific, distribution channel-specific or user-specific basis depending upon the attainment of a valid license. Users can also be provided with an application that allows them to browse or search for items in aggregated datasets, and to purchase selected items via a transaction involving the computer-dependent product code and activation code. This Protexis model also allows for downstream rights acquisition and delivery – rights delivered or modified subsequent to the initial delivery or enablement. Additional rights may be granted or restricted in conjunction with an update or upgrade to the dataset or software.

Authentication & Integrity

Authentication of content sources and authentication of users are both important aspects of any technological protection system. In some cases, it is necessary to verify both the source of content and that it has not been altered before the user views it. For example, assume that a medical text, containing medicinal dosage amounts (among other things), is distributed with a technological protection system. It would be in the interest of the publisher and users to ensure that the medical text and, especially, the dosage amount are not altered. Content source authentication ensures that this cannot occur without detection.

User authentication verifies the identities of users who want to access and use content. This could take the form of a password, a cookie on a user's machine, a token incorporating a cryptographic algorithm, biometrics, or other technology-based tracking solutions. Through activation-based systems, locking the content use or access to a specific computer provides a convenient and robust user authentication methodology. With these technologies, users do not have to validate themselves (*e.g.* enter a password every time they initiate previously authorized use of a program or view content) and the computer can automate this task itself. Such computer authentication systems can be readily combined with user authentication systems so as to seamlessly incorporate the advantages of both.

Certain authentication models (such as Protexis' nTitles system) provide content publishers and distributors with choices for authentication such as activation only, activation with optional registration, or activation with mandatory registration. Activation employs computer-dependent product codes for user integrity verification.

Beyond user authentication and content integrity, the rights model and the license terms themselves require authentication and integrity validation for current, as well as subsequent use.

For example, in the nTitles system data elements critical to the operation of a software program can be encrypted and subject to different license terms. The data elements can then be searched for installed licenses. A valid license is needed to decrypt a corresponding data element and reveal it; otherwise, the software program operates sub-optimally. In this type of system, license terms validation and computer (i.e., user) authentication is normally automated within this rights system.

Secure Containers/Wrappers

Many technological protection system schemes include a "secure container" (sometimes called a "digital wrapper") that protects content from unauthorized access by holding it in an encrypted form until appropriate "keys" are used to open it. Secure containers include information (metadata) about the content—generally the rules, based on rights models (see above) under which users can access it. Users go through an authentication process to access the content; then the content is "unwrapped" and presented in its native state (HTML, Word document, etc.)

For example, suppose an MP3 digital music file is purchased online. The MP3 file is wrapped with an encryption device that protects it during shipment. The music publisher, or its designated service provider, executes a digital license -- or key -- for consumers that allows them to unwrap the MP3 file. Once the file is unwrapped, the consumer is bound by the terms and conditions of the license, which may allow him or her to play the file on the PC, download it to an external player or transfer it to a CD.

Most technological protection systems with secure containers do not give the user access to a "naked" (copyable) file after authentication. Instead, they provide a piece of client software that displays or plays the content in a restricted fashion, prohibiting things like printing and making a file copy. Such systems are not 100 percent foolproof, but they act as strong deterrents to unauthorized copying.

For the image market, developers of the upcoming JPEG2000 image file format are investigating secure container technologies. ISO and DIG (the Digital Imaging Group – http://www.digitalimaging.org) are discussing a file format that includes a mandatory form of metadata containing rights information referred to as a "license plate" for each image. A JPEG2000-compliant web browser would first read the license plate and then decide if that image could be displayed on a page depending upon where, or who, was viewing the page. Other rights, such as the right to copy the image from the web page would also be controlled or accessed through the license plate.

Some technological protection systems use hardware technology, instead of (or in addition to) software, to protect content. These are somewhat like the "dongles" that software vendors use to authenticate users' PCs and prevent unauthorized use. This type of technological protection system requires that users install special devices in their PCs or in some cases purchase PCs with such devices pre-installed. These are the most secure devices, but users often dislike them intensely, and they are only used on the most expensive types of software content.

Macrovision's wrapper technology, called SafeWrap™, employs a variety of technologies including secure encryption, obfuscation, debugger detection, and other proprietary techniques.

When applied to software files in combination, these methods block hackers from examining executable code, and ensure that applications that have been tampered with or modified will not run. SafeWrap is designed to protect code against hacking, tampering, and reverse engineering. SafeWrap is updated regularly to incorporate new protective strategies and keep pace with hackers' latest tactics. If software protects, distributes, or allocates valuable digital assets or content, SafeWrap blocks hackers from assigning themselves additional rights or access privileges without authorization

Clearinghouses

Clearinghouses provide a single-source entity for management of reproduction rights for many different content providers. Clearinghouses also meter usage of content and, when appropriate, initiate e-commerce transactions so those users can pay for rights.

In addition, clearinghouses can record and compile specific information about content usage. Such information is, in many cases, of more value than any price that a publisher might charge for access to content. The collection of data created by consumers' interactions with content can help publishers build knowledge and understanding of their particular market and adopt new marketing models. For example, an online information publisher adopts a "daily push" model, distributing thousands of pieces of information to businesses worldwide. A sophisticated back-office system collects usage audit records from these businesses and utilizes data mining capabilities so that the publisher knows what types of information its business customers actually use. From this knowledge, the publisher better segments its customers and provides more targeted services.

One example of a clearinghouse is Copyright Clearance Center ("CCC"). CCC has bilateral contracts with almost 20 counterpart organizations in other countries. CCC is the largest licensor of rights for academic paper coursepacks in the U.S. through its Academic Permissions Service. CCC is also the largest third-party licensor in the U.S. of electronic access to coursepack-type materials for education in colleges and universities through its Electronic Course Content Service.

CCC's Rightslink™, an enterprise software solution for publishers to license and deliver digital content, gives end-users access to content while giving publishers the ability to secure and monetize their digital content. Publishers can use this technological protection system to grant permissions, deliver digital content, automatically generate paper reprints, and secure high-value content. Rightslink is comprised of several separate but integrated modules called the Permissions, Security, Reprints and Metrics modules. The Permissions module allows a publisher to set the business rules for the reuse of their content. For example, emailing an article might be free; republishing it in a brochure might cost $10 per copy, while republishing it in a competing publication might only be allowed after 30 days after the first printing, for $1000. The Security module protects sensitive or high-value content. Designed to prevent the unlawful distribution of intellectual property, it lets the publisher control distribution of text, images, and photography. For example, the security module allows content to be viewed in a standard web browser but prevents it from being saved, forwarded, printed, or screen captured without proper authorization. The Reprints module lets publishers automate requests for reprints, either electronic or paper-based. Lastly, the Metrics module provides publishers with reporting and tracking on the ways end users are using content, subject to user consent.

iCopyright is another clearinghouse. iCopyright provides "The Instant Clearance Service," an automated content licensing engine for text-editorial content, including any photos, graphs, and charts that accompany articles. The system can incorporate various encryption wrappers at the option of the content owner. Upon request, iCopyright presents the reader with various licensing options (as set by the owner), then allows the reader to purchase the license and instantly receive the content in the desired format. Secure Display Technology allows any piece of text-editorial content to be viewed and read, but makes it impossible to print, cut, copy, paste or screen capture the material without first obtaining a proper license. Before material can be legally licensed and before it is provided in a better-designed version, a license number and tracking ID is embedded in the content to prove compliance and the user's record of clearances is stored in perpetuity. iCopyright has tagged more than five million articles and issued more than 50,000 licenses. Each month, 250,000 new pieces of content are tagged by the iCopyright system for instant licensing and copyright compliance. The user's record of clearances is stored in perpetuity so that he/she may return to examine the material at any time.

2. What systems have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad-based consensus process?

A brief summary of various industry initiatives is provided below.[2] There is much being done in this area so we strongly urge you to find out more about these initiatives by checking the newest information on individual project websites.

XrML -- Extensible Rights Markup Language: "The Digital Rights Language for Trusted Content and Services." XrML provides a universal method for securely specifying and managing rights and conditions associated with all kinds of resources, including digital content as well as services. In addition, standards such as XSLT and XPath have been employed in XrML, and XML Signature and XML Encryption have been used for authentication and protection of the rights expressions. For details, see www.xrml.org or www.contentguard.com

Information and Content Exchange (ICE) is a protocol that supports content syndication, i.e., automated piecemeal licensing of content over the Internet. Its development is overseen by an authoring group that includes Vignette Corp., Microsoft, Sun Microsystems, Adobe and several other technology and media companies. ICE-based content syndication applications are intended to automatically transfer content and rights from one organization to another in a trusted relationship, where terms are enforced by written contract instead of by technology. For details, see http://www.vignette.com/CDA/Frameset/0,1031,S1-L1-Book-173,FF.html.

[2] The inclusion or exclusion from this list of an industry initiative should not be construed as SIIA's endorsement or disapproval of any particular initiative. SIIA provides this list for information purposes only.

The Digital Object Identifier (DOI) is used to record and return content and present links to multiple related materials (for example, articles, books, images, bibliographies, supporting data, videos, charts, tables, and audio and electronic files). In the fast-changing world of content production, ownership of information, and location of electronic files, rights and related material change frequently over the life of a work. Using the DOI enables persistent resolution to this multitude of changing information with one keystroke and ensures that users across the supply chain are always presented with the correct information. A registered not-for-profit foundation, DOI created a system that integrates a persistent identifier of intellectual property entities (creations), a reliable resolution system, and associated metadata that enables the construction of services in the digital environment. The DOI is now being used in large-scale implementations, with more applications under development. See http://www.doi.org/about_the_doi.html

The Organization for the Advancement of Structured Information Standards (OASIS) established a Rights Language Working Group in mid-2002. OASIS is a not-for-profit, global consortium that develops standards largely based on XML. The goal of the Technical Committee is to define the industry standard for a rights language that supports a wide variety of business models and has an architecture that provides the flexibility to address the needs of the diverse communities that have recognized the need for a rights language. The language needs to be: comprehensive -- capable of expressing simple and complex rights; generic -- capable of describing rights for any type of digital content or service; precise – able to communicate precise meaning to all components of the system; interoperable -- able to comprehend it is part of an integrated system; and agnostic to platform, media type or format. More information on OASIS can be found at: http://www.oasis-open.org/committees/rights/

The PAIDFAIR project: The goal of PAIDFAIR ("Protecting Accumulated Intellectual Data for Accounting in Real-Time," IST-2000-29616 -- which is partly supported by the European Commission -- is to set a worldwide standard for payment for intellectual property content or software use. The objectives are demonstration systems in fields of secure electronic software distribution and Pay-Per-Use, distribution of music content, e-payment and authentication integration with Smart Card, IP Distribution through broadcast/multicast and satellite communication, biometrical authentication and secure downloads for open Multimedia Home Platform (MHP) set-top-box. The PAIDFAIR trial intends to adapt and introduce the new leading edge encryption technology CodeMeter. More information about PAIDFAIR can be found at: http://www.paidfair.com/us/index.php

The Shared Content Object Reference Model (SCORM) defines a Web-based learning "content model." It includes a set of interrelated technical specifications designed to meet the Department of Defense's high level "-ilities", providing a bridge from general emerging technologies to commercial implementations. Developed by ADL - Advanced Distributed Learning – this group can be reached at http://www.adlnet.org

The Moving Picture Experts Group (MPEG) is a working group of ISO/IEC, JTC 1 / SC 29 / WG 11 in charge of the development of international standards for compression, decompression, processing, and coded representation of moving pictures, audio and their combination. The rights language is expected to reach final committee draft in December 2002. The final draft of the ISO standard is expected by the summer of 2003. More information on MPEG can be found at: http://mpeg.telecomitalialab.com/

The Open eBook Forum (OeBF) is an international trade and standards organization for the electronic book (e-book) industry. The Open eBook Publication Structure (OEBPS) is an open, non-proprietary, XML-based specification for the content, structure, and presentation of electronic books. OEBPS is maintained by the Open eBook Forum (OeBF), a group of many organizations involved with, or interested in, electronic publishing and related areas. Members include hardware and software companies, publishers, authors, users of e-books, and related organizations whose common goals are to establish specifications and standards for electronic publishing. More information on the OeBFPS can be found at: http://www.openebook.org/oebps/index.htm

Copy Protection Technical Working Group (CPTWG) is comprised of content providers, consumer electronics manufacturers, and information technology companies. Its aim is to seek consensus on technological solutions for various content protection challenges, including protecting the new business opportunity in the DVD home video market from casual piracy. The CPTWG began by launching an encryption approach called Content Scrambling System (CSS) in 1997. More information on the CPTWG can be found at: http://www.cptwg.org

DVD Copy Control Association (DVD CCA) is a not-for-profit corporation with responsibility for licensing CSS (Content Scramble System) to manufacturers of DVD hardware, discs and related products. Licensees include: owners and manufacturers of the content of DVD discs; creators of encryption engines, hardware and software decrypters; and manufacturers of DVD Players and DVD-ROM drives. More information on the CPTWG can be found at: http://www.dvdcca.org/

The Universal Description, Discovery and Integration (UDDI) protocol creates a standard interoperable platform that enables companies and applications to quickly, easily, and dynamically find and use Web services over the Internet. UDDI also allows operational registries to be maintained for different purposes in different contexts. UDDI is a cross-industry effort driven by major platform and software providers, as well as marketplace operators and e-business leaders within the OASIS standards consortium. More information about UDDI can be found at: http://www.uddi.org/

The TV-Anytime Forum is an international association of organizations that seeks to develop specifications to enable audio-visual and other services based on mass-market high volume digital storage in consumer platforms. The TV-Anytime Forum is developing a standard for the secure and flexible expression and enforcement of rights holders' usage conditions for media distributed to personal digital recorders. Its fundamental goals include establishing means of securely enabling diverse leading edge consumer content usage models while providing standardized interfaces to legacy conditional access and content protection systems. More information about the TV-Anytime Forum can be found at: http://www.tv-anytime.org/

The Publishing Requirements for Industry Standard Metadata (PRISM) is an extensible XML metadata standard for syndicating, aggregating, post-processing and multi-purposing content from magazines, news, catalogs, and mainstream journals. PRISM provides a framework for the interchange and preservation of content and metadata. PRISM also provides a set of controlled vocabularies with which to describe the content being interchanged, thereby providing a common interchange that should expand the market for licensed content. More information about PRISM can be found at: http://www.prismstandard.org/

The Internet Streaming Media Alliance (ISMA) is a non-profit corporation formed to provide a forum for the creation of specification(s) that define an interoperable implementation for streaming rich media (video, audio and associated data) over Internet Protocol (IP) networks. ISMA is an alliance that is comprised of companies that deliver solutions for the complete value chain of authoring, encoding, capturing, managing, distributing, streaming and consuming media. ISMA builds upon existing ratified standards to endorse an implementation specification for delivering streaming rich media over IP protocols. More information about ISMA can be found at: http://www.isma.tv/

The Object Management Group (OMG) is an open membership, not-for-profit consortium that produces and maintains computer industry specifications for interoperable enterprise applications. The OMG was formed to create a component-based software marketplace by hastening the introduction of standardized object software. The organization's charter includes the establishment of industry guidelines and detailed object management specifications to provide a common framework for application development. More information about OMG can be found at: http://www.omg.org

The two most basic and important groups defining public standards for the Internet are:

The Internet Engineering Task Force (IETF) is an open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. The IETF addresses intellectual property issues by documenting existing publishing practices and identifying what practices need alteration. More information about IETF can be found at: http://www.ietf.org/

The World Wide Web Consortium (W3C) develops interoperable technologies (specifications, guidelines, software, and tools) for the World Wide Web. In the intellectual property area, W3C's goal is to make it easier for users to obey the law by combining payment and labeling technologies to clearly express the terms and conditions related to online materials and to make it easier to stop indiscriminate redistribution of protected material by establishing a labeling system for cataloging sites that are known to contain infringing materials. More information about W3C can be found at: http://www.w3.org/

3. **Consistent with the types of information requested by Congress, please provide any additional comments on technological protection systems to protect digitized copyrighted works and prevent infringement.**

Because the Federal Register notice is responsive to a requirement in the TEACH Act, it is important to discuss the use of technological protection systems by educational institutions.

Educators, content providers, policymakers and the high-tech industry have been partnering for more than two decades to bring the benefits of computer technology to the classroom. While the integration of technology as a teaching tool has been a gradual process, students of all ages are reaping benefits at an exponential rate due to the increasing ubiquity of the Internet. As a result, the evolution of computer technology in the educational environment is revolutionizing educational perceptions, practices and structures. Technology is changing both the process, and the business, of education.

Technology can challenge long-standing education models by increasing choice and empowerment. It can also simultaneously expand and reduce risks associated with illegal re-distribution and misuse of copyrighted materials originally used for educational purposes. Responding to the potential of distance education and the need to protect proprietary content used in distance education programs and elsewhere, SIIA member companies and many other high-tech companies have made considerable technology investments in recent years.

Every day new and improved technologies are being developed to protect copyrighted content from piracy. Just as educational institutions have integrated technologies into teaching and learning to facilitate delivery of course curricula, under the TEACH Act they now must also integrate technological protection systems into their distance education programs to protect copyrighted works used in those programs. This requirement was an essential component of the TEACH Act.

Without the use of robust, effective technological protection systems, the copyrighted educational content used in distance education programs is likely to be illegally distributed and/or misused by students enrolled in the programs as well as others who may gain unauthorized access. When educators take advantage of new technologies to encourage students to use and access copyrighted content, they must keep in mind that end users generally do not know or do not care about protecting the copyrighted content.

Most (87.9 percent) of the college administrators from 632 institutions surveyed by Campus Computing reported having a written policy regarding software duplication. Despite the best intentions of these educational institutions, student software piracy rates remain high. A recent study by the *Student Monitor* found that, in 2002, 46% of college undergraduate students obtain their software illegally from family or friends. This number is down only slightly from the 2001, when 49% of college undergraduate students obtained their software illegally.[3] The 2002 study also showed that 34% of the students visited Kazaa to acquire software or for other reasons.[4]

These studies show that it is essential that any copyrighted content used in distance education programs be protected by robust, effective technological protection systems. As any business can attest, technology costs are a dynamic budget item, requiring continued investment in infrastructure, software, support and training. Accordingly, accredited nonprofit educational institutions wishing to take advantage of the new distance education exception under the TEACH

[3] *See* http://www.studentmonitor.com/f02ci

[4] *id.*

Act should take steps to ensure that they: (1) use technological protection systems to protect any copyrighted content used in a distance education program; (2) budget for such technologies; and (3) continuously monitor the effectiveness and the success rate of the technology used. The TEACH Act was passed with the implied and expressed understanding that the benefits to accredited nonprofit educational institutions come with a set of shared responsibilities in the form of the requirement to employ technological protection systems.

Request to Testify

If the PTO decides to hold hearings on "Technological Protection Systems for Digitized Copyrighted Works, SIIA hereby requests to testify at such hearings.

Conclusion

In closing, we would once again like to thank the PTO for giving us the opportunity to provide our comments. Should the PTO have any questions or concerns about the statements made in this letter, we would be pleased to expand upon them. We look forward to testifying at the upcoming hearings on this matter.

Respectfully submitted,

Ken Wasch

Ken Wasch
President
Software & Information Industry Association

APPENDIX A

List of Technological Protection System Providers

The companies listed below offer technological protection system solutions to rights-holders and education providers that distribute content electronically, either on the Internet or by other means. SIIA does not endorse these companies or their products, but identifies them as a resource for the U.S. Patent and Trademark Office, Copyright Office, and education providers.

COMPANY	WEB SITE	PRODUCT EXAMPLES[5]
Adobe Systems	www.adobe.com	Content Server
Alchemedia	www.alchemedia.com	Mirage
Aladdin Knowledge Systems	www.ealaddin.com	HASP, eToken, Privilege
Authentica	www.authentica.com	PageRecall, NetRecall
Axeda	www.axeda.com/solutions/index.html	Axeda Device Relationship Management System
BayTSP	www.baytsp.com	BayTSP
Blue Spike	www.bluespike.com	Giovanni digital watermarking system
Cloakware Corp.	www.cloakware.com	Cloakware/Transcoder
ContentGuard	www.contentguard.com	XrML
Copyright Clearance Center	www.copyright.com	RightsLink
Cyveillance	www.cyveillance.com	Digital Asset Management
Datamark	www.datamark.co.uk	Datamark
Digimarc Corporation	www.digimarc.com	ImageBridge, MarcSpider, Security Class
Digital Rights LLC	www.digitalrightsllc.com	DRM Lite
Digital World Services	www.dwsco.com	ADo^{2}RA^{sm}
DigiTreal	www.digitreal.com	WaterStamp, PaVi

[5] Most of the products listed below are registered trademarks or servicemarks.

COMPANY	WEB SITE	PRODUCT
DotEncrypt	www.dotencrypt.com	dotEncrypt Publisher
Element5 AG	www.element5.com	element 5
Elisar Software	www.clisar.com	MediaRights
eMeta Corp.	www.emeta.com	eRights
FileOpen	www.fileopen.com	FileOpen Publisher
GenuOne	www.genuone.com	GenuGuard, GenuNet
IBM	www.3.ibm.com/software/data/emms	Electronic Media Management System (EMMS)
iCopyright Inc.	www.icopyright.com	Insant Clearance Service
Info2clear	www.info2clear.com	get-a-copy, get-a-song, get-a-seal,
InterTrust Technologies Inc.	www.intertrust.com	Rights|System, RightsPD
LockStream	www.lockstream.com	Secure Package Creator, Secure Package Reader
Macrovision	www.macrovision.com	MacroSafe, SafeDisc, FlexLM, MacroSAFE, Safe Authenticate, SafeCast, SafeWrap, SAM Solutions, GT Licensing, Cactus Data Shield
Markany Corp	www.markany.com	ContentSafer, MAVI, MarkAny, MAO
MediaDefender	www.mediadefender.com	P2P Anti-Piracy technologies
MediaForce	www.mediaforce.com	MediaSentry, MediaExchange, MediaDecoy
Microsoft	www.microsoft.com/windows/windowsmedia/drm.asp	Windows Media DRM
Ness Technologies	www.ness-europe.com/iRights/Default.htm	iRights
NetActive Inc.	www.netactive.com	Reach
NetPD	www.netpd.com	Internet searches
NetQuartz	www.netquartz.com	ez Platform
Overdrive	www.overdrive.com	Overdrive DRM Solutions
PACE Anti-Piracy	www.paceap.com	Ilok, Satisfaction
Perico AS	www.pericosecurity.com	Sentinel Hardware Keys
Phocis	www.phocis.com/	Secure Digital Xchange, Secure Publishing Xchange

COMPANY	WEB SITE	PRODUCT
Protexis Inc.	www.protexis.com	nTitles
Rainbow Technologies	www.rainbow.com	iKey, SentinelLM, CryptoSwift, NetSwift
RangerOnline Inc.	www.rangerinc.com	Internet Searching
RightsMarket Inc.	www.rightsmarket.com	RightsEnforcer
SealedMedia Inc.	www.sealedmedia.com	SoftSEAL, License server, Sealer, Unsealer
ShieldIP	www.shieldIP.com	ShieldIP
Smarte Solutions	www.smartesolutions.com	SmarteSecure, SmarteKey
Softwrap Limited	www.softwrap.com	Softwrap, Soundwrap
Sospita	www.sospita.com	SecureWeb
SunnComm	www.sunncomm.com	MediaCloq
Syncast	www.synccast.com/pages/products/DRM/default.htm	Syncast DRM Dashboard, Syncast DRM Packager
Verance	www.verance.com	Content Owner Embedding Packages
Vidius	www.vidius.com	PortAuthority, NetGuard, PA/ClearSite
WIBU-Systems AG	www.wibu.com	WIBU-Key, SmartShelter, CodeMeter
z4 Technologies	www.z4.com	z4security, z4security plus

APPENDIX B